ABSTRACT

A time period which is expended since a request for the authentication of the validity of a public key certificate till the authentication of the validity, is shortened. A certificate validity authentication center VC periodically searches for and verifies paths which extend from a bridge certification authority CA$_{bridge}$ to individual terminal admitting certification authorities CA, and it registers the paths whose verifications have held good, in a path database in association with the respective terminal admitting certification authorities CA. Besides, in a case where the request for the authentication of the validity of a certificate has been made by an end entity EE, whether or not a path associated with the terminal admitting certification authority CA which admits the end entity, and a path associated with the terminal admitting certification authority CA which has issued the certificate being a subject for the request are registered in the path database is checked, and the subject certificate is judged valid only when both the paths are registered.